UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

SUSAN WINSTEAD, individually and on behalf of all similarly situated persons, Plaintiff, v. COMPLYRIGHT, INC., a Minnesota corporation, Defendant.	**Civil Action No. 1:18-cv-4990** **CLASS ACTION** **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Susan Winstead ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to her and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against defendant ComplyRight, Inc. ("ComplyRight" or "Defendant").

NATURE OF THE ACTION

1. Plaintiff brings this class action against ComplyRight for its failure to implement and maintain reasonable security measures over personally identifiable information—in particular, their name, address, telephone number, email address, and Social Security number (the "Personal Information").

2. On July 13, 2018, ComplyRight sent letters to Plaintiff and many others around the country informing them that their name, address, telephone number, email address, and Social Security number (the "Personal Information") were accessed and viewed by unauthorized individuals while being maintained on ComplyRight's website (the "Data Breach"). The letter warned recipients that "your personal information that was accessed and/or viewed, [] may have

been downloaded or otherwise acquired by an unauthorized user." The letter admits that the Data Breach occurred from April 20, 2018 to May 22, 2018, but it may have gone on much longer, and it may have exposed more information than enumerated in the letter.

3. The letter also explained how ComplyRight came to be in possession of Plaintiff's sensitive personal information: "Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2."

4. On information and belief, as a result of the Data Breach, Plaintiff's and the other Class members' Personal Information, and perhaps more information, is now in the hands of unknown persons who intend to use it for criminal or nefarious purposes. On information and belief, the unauthorized persons will sell the Personal Information to exploit and injure Plaintiff and the other Class members, to commit identity theft and identity fraud, and commit other acts injurious and detrimental to Plaintiff and the other Class members.

5. Criminals use information like the Personal Information to commit various crimes, such as opening fraudulent credit accounts in the name of the victim, file a fraudulent income tax return and divert any refund to the criminal's bank account, and impersonate the victim when arrested, when obtaining medical services, and seeking employment. These crimes cause significant harm to the victims that can last for years.

6. The Data Breach was caused and enabled by ComplyRight's violation of its obligations to implement and maintain reasonable security measures to protect Personal Information from unauthorized access, acquisition, destruction, use, modification and disclosure and provide timely, adequate, and non-misleading notification of the Data Breach under the

common law, the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2 and 505/2RR, and the Personal Information Privacy Act, 815 Ill. Comp. Stat. 530/45.

PARTIES

7. Plaintiff resides within the Northern District of Illinois, and is a citizen of the State of Illinois. On July 17, 2018, she received a letter from ComplyRight informing her that her Personal Information was accessed and/or viewed by unauthorized persons from its website.

8. Defendant ComplyRight, Inc. is a Minnesota corporation with its principal place of business in Pompano Beach, Florida.

JURISDICTION AND VENUE

9. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events and omissions giving rise to these claims occurred in this District.

FACTUAL BACKGROUND

11. ComplyRight offers a suite of legal compliance services for small businesses. On its website, it states: "At ComplyRight, our mission is to free employers from the burden of tracking and complying with the complex web of federal, state, and local employment laws, so they can stay focused on managing and growing their businesses." Their services range "[f]rom hiring and training to time tracking and recordkeeping, to labor law posting and tax information reporting."

12. In order to engender trust with potential clients, ComplyRight touts its security and industry and regulatory certifications.

13. Its website, located at https://www.complyright.com/products/tax-solutions (last visited July 19, 2018), displays the following:

14. ComplyRight's website boasts about its State of the Art Encryption: "As a leading IRS-authorized provider of 1099, W-2, and ACA form processing services, we employ the latest, most sophisticated technologies and best practices to ensure your sensitive data is protected end-to-end. These exacting measures and adherence to strict security standards ensure a superior level of data security and protection."

15. The site also states:

> ComplyRight Tax Solutions uses advanced 256-bit encryption technology to block the interception of sensitive data over the internet. Encryption alters the data before it is transmitted, making it unreadable until it is unlocked with a special cyber code after it is delivered to the authorized recipient. Data is password-protected and encrypted as soon as it's entered online and stays encrypted through the entire print, mail, and e-file process.
>
> - High-grade transport encryption protects electronic transmissions to the IRS and other government agencies
> - Includes encryption at rest to safeguard information stored in our systems

- Effectively blocks interception of sensitive data

16. The website also boasts about its SOC-2 certification, stating,

As a SOC-2-certified organization, we can promise:

- Security – Our system is protected against unauthorized access, use, or modification
- Availability – Our system is available for operation and use as committed or agreed upon
- Processing integrity – Our data processing complete, valid, accurate, timely and authorized
- Confidentiality – confidential information is protected as committed or agreed upon
- Privacy – Our processes for collecting, using, retaining, disclosing, and disposing of personal information conform with the commitments in our privacy notice, and with criteria established by the AICPA.

17. ComplyRight runs the website efile4biz.com, which also boasts state-of-the-art security. In order to convey the strength of its security, it says it is Geotrust and SOC certified, in HIPAA compliance, and authorized as an IRS e-file provider.

18. The website pays lip service to the need for adequate security to protect against the cyber threats facing its business, but only to lure potential clients:

> Due to the increasing threat of data breaches and identity theft in today's digitally focused world, you may question the security of e-filing. . . . As an industry leader and pioneer in online 1099, W-2, and ACA form processing, we employ the latest, most sophisticated security measures. The result is a level of data protection that would thwart even the most determined cyber criminals.
>
> . . .
>
> When it comes to risk-free e-filing, be aware that the IRS doesn't regulate how recipient data is handled. Instead, it's entirely up to the service provider. In turn, it's up to you to ask the right questions to be certain you're entrusting your 1099, W-2 and ACA recipient data to a security-conscious provider.

19. Plaintiff and the other Class members had their Personal Information entrusted in the wrong hands. Despite these assurances and representations, ComplyRight failed to implement

and maintain reasonable data security practices in accordance with its representations and the obligations it owes under the law.

20. On July 13, 2018, ComplyRight sent a letter out to Plaintiff and numerous other persons stating in part:

> We are writing with important information about a recent security incident involving some of your personal information that was maintained on our website. Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2. We wanted to provide you with information regarding the incident, share the steps we have undertaken since discovering the incident, and provide guidance on what you can do to protect yourself.
>
> *What Happened?*
>
> On or about May 22, 2018 we initially learned of a potential issue involving our website. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website.
>
> *What We Are Doing*
>
> In addition, we commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to our website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of our website, and analysis of potentially impacted individuals, on June 14, 2018 we discovered that some of your personal information was accessed and/or viewed. Although the forensic investigation determined that your information was accessed and/or viewed on the website, it could not confirm if your information was downloaded or otherwise acquired by an unauthorized user. We are not aware of any report of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution we wanted to make you aware of the incident.
>
> *What Information Was Involved?*
>
> Your personal information that was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user included your name, address, telephone number, email address, and Social Security number.[1]

[1] By quoting from ComplyRight's letter, Plaintiff does not intend to endorse the representations, nor concede in any way that the representations made therein are accurate or true. They are quoted merely to show that the statements were made and Plaintiff received them.

21. On information and belief, Plaintiff and the other Class members' Personal Information was accessed, viewed, downloaded, acquired, and stolen by unauthorized persons from ComplyRight's website. The letter leaves open the possibility that other information was also compromised.

22. The letter is insufficient to comply with ComplyRight's obligations to provide adequate and timely notification of the Data Breach under the law. ComplyRight awaited a sophisticated and extensive forensic investigation when timely notification of the Data Breach was of the essence. ComplyRight kept the incident secret from Plaintiff and the other Class members for nearly 2 months. Data thieves had 3 months from the alleged beginning of the Data Breach until notification to perpetrate fraud using the Personal Information with no victim aware of the threat.

23. The letter did not identify the number of affected individuals. However, Plaintiff has reason to believe that the number of impacted individuals is very large.

24. In a 2017 news release, ComplyRight boasted that it "has partnered with millions of businesses of all sizes."

25. Impacted individuals from around the country took to social media to raise concerns and questions about ComplyRight's confusing and concerning letter. ComplyRight's failure to provide any details to trusted news media or on its own website concurrently with the issuance of the letter created confusion and distrust among letter recipients, who largely have no idea who or what ComplyRight is, and suspect that the letter is fraudulent because they can find no mention of the incident online or in the news.

26. By all appearances, ComplyRight refuses to respond to concerned individuals or news media, except through a heavily backlogged call center.

27. It did not take long for misinformation to spread online. Theories abound about the actual nature of the breach, whether it is legitimate or not, whether it is associated with other entities, or whether their employers ever actually used ComplyRight or any third party services related to tax preparation at all. This misinformation that filled in the void of ComplyRight's silence allows for phishing and other scams to seize advantage of those already victimized by the Data Breach.

28. Justifiably wary of scams, some victims report spending an entire day attempting to confirm that the Data Breach was legitimate and uncover new details. For instance, an individual posted to the subreddit r/personalfinance:[2]

> I did further research, called the company hotline provided as well as the company directly, called TransUnion, spent a day calling everyone. There was a real hack, it does not sound like it was Turbotax (this was something the customer service person from ComplyRight told me). ComplyRight handles employer end e-filing, not employee. So, the information was entered by your employer, and then hacked through ComplyRight. Honestly I'm very disappointed with the hotline provided by ComplyRight. The first thing they do is ask for more private information, and honestly they basically just read the letter off to me over and over again.
>
> TransUnion confirmed that they own the website mytrueidentity.com, which is the url provided in the letter. I signed up for the service, which now I'm thinking I shouldn't have because I imagine it waives my right to any other sort of recourse. If anyone else is able to get more information, please provide it!

29. Late Wednesday, July 18, 2018, only after Plaintiff and a substantial number of other recipients received their letters, did ComplyRight provide largely the same information in an inconspicuous and difficult to access webpage on its website establishing some sort of authenticity to the letter, but by then it was too little too late.

30. As a direct and foreseeable result of ComplyRight's failures, Plaintiff and the other Class members' Personal Information was placed onto unsecure and vulnerable online locations

[2] https://www.reddit.com/r/personalfinance/comments/8zeeha/information_stolen/

maintained by ComplyRight. The Personal Information (and perhaps more) was accessed, viewed, obtained, downloaded, and is now in the hands of unknown individuals intent on using the information to harm Plaintiff and the other Class members.

Data Breaches Lead to Identity Theft

31. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[3]

32. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

33. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[5] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

[3] See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[5] Companies, in fact, also recognize Personal Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

34. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[6]

The Monetary Value of Privacy Protections and Personal Information

35. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[7]

36. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[8]

37. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[9]

---

[6] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at https://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited July 19, 2018).

[7] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited July 19, 2018).

[8] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[9] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited July 19, 2018).

38. Recognizing the high value that consumers place on their Personal Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their personal information.[10] This business has created a new market for the sale and purchase of this valuable data.[11]

39. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[12]

40. The value of Plaintiff's and Class members' Personal Information on the black market is substantial. By way of the Data Breach, ComplyRight has deprived Plaintiffs and Class members of the substantial value of their Personal Information. Rather than have an unknown third party realize the value of her Personal Information, Plaintiff would choose to realize that value herself.

Damages Sustained by Plaintiff and the Other Class Members

41. Plaintiff and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper

[10] Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited July 19, 2018).

[11] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[12] *See* Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

disclosure of their Personal Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) the value of their time and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud; and (v) deprivation of the value of their Personal Information, for which there is a well-established national and international market.

42. Plaintiff and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

43. Acknowledging the damage to Plaintiffs and Class members, ComplyRight is instructing consumers to "remain vigilant in reviewing . . . financial account statements and credit reports for fraudulent or irregular activity." Plaintiff and the other Class members now face a greater risk of identity theft.

CLASS ALLEGATIONS

44. Plaintiff brings Count I, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Nationwide Class") defined as:

> All persons whose Personal Information was contained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

45. Plaintiff brings Counts II–IV set forth below on behalf of herself and a statewide class for Illinois (the "Illinois Class") defined as:

> All persons residing in Illinois whose Personal Information was contained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

46. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

47. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** Class members are so numerous that joinder of all Class members would be impracticable. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from ComplyRight's and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

48. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether ComplyRight failed to use reasonable care and reasonable methods to secure and safeguard Plaintiff's and the other Class members' Personal Information;

b. Whether ComplyRight properly implemented its purported security measures to protect Plaintiff's and the other Class members' Personal Information from unauthorized capture, dissemination, and misuse;

c. Whether ComplyRight took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether ComplyRight provided timely and adequate notification of the Data Breach after it first learned of same;

e. Whether ComplyRight willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Personal Information;

f. Whether ComplyRight was negligent in failing to properly secure and protect Plaintiff's and the other Class members' Personal Information;

g. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

49. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

50. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. There are no defenses available to Defendant that are unique to Plaintiff.

51. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other Class members she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously.

The other Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

52. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against ComplyRight, so it would be impracticable for Class members to individually seek redress for ComplyRight's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

COUNT I
Negligence
(On Behalf of the Nationwide Class)

53. Plaintiffs incorporate paragraphs 1–52 as if fully set forth herein.

54. ComplyRight owed numerous duties to Plaintiff and the other members of the Class. These duties include the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Personal Information in its possession;

b. to protect Personal Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices and the practices and certifications represented on its website which it voluntarily undertook duties to implement; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly and sufficiently notifying Plaintiff and the other members of the Class of the Data Breach.

55. ComplyRight, a purported expert in legal compliance, knew or should have known the risks of collecting and storing Personal Information and the importance of maintaining secure systems. ComplyRight knew of the many breaches that targeted other entities in the years preceding the Data Breach, as illustrated by its own representations alleged herein.

56. Given the nature of ComplyRight's business, the sensitivity and value of the information it maintains, and the resources at its disposal, ComplyRight should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

57. ComplyRight knew or should have known that its systems did not adequately safeguard Plaintiff's and the other Class members' Personal Information.

58. ComplyRight breached the duties it owed to Plaintiffs and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols and practices sufficient to protect Personal Information and thereby creating a foreseeable, unreasonable risk of harm;

b. by failing to comply with the minimum industry data security standards and its own assurances of superior data security standards;

c. by negligently performing voluntary undertakings to secure and protect the Personal Information it solicited and maintained; and

d. by failing to timely and sufficiently discover and disclose to consumers that their Personal Information had been improperly acquired or accessed, and providing misleading and unfounded suggestions that their information (and by extension their identity) is not in the immediate peril it is in fact in.

59. But for ComplyRight's wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, their Personal Information would not have been compromised.

60. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of ComplyRight's negligent conduct. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

61. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the common law duties enumerated above, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II
Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2
(On Behalf of the Illinois Class)

62. Plaintiff incorporates and realleges paragraphs 1–52 as if fully set forth herein.

63. Plaintiff and the other members of the Class were subjected to ComplyRight's unfair or deceptive acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the Data Breach.

64. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

65. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at last one month, and perhaps longer.

66. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

67. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

68. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

69. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22,

2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through media or on its website (and by all appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

70. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

71. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

72. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the Illinois Consumer Fraud Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

73. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT III
Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2RR
(On Behalf of the Illinois Class)

74. Plaintiff incorporates paragraphs 1–52 as if fully set forth herein.

75. ComplyRight violated 815 Ill. Comp. Stat. 505/2RR(a)(1) by publicly posting or publicly displaying in any manner Plaintiff and the other Class members' social security number.

76. ComplyRight violated 815 Ill. Comp. Stat. 505/2RR(a)(3) by requiring social security numbers to be transmitted over the internet without a secure connection or requiring encryption.

77. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

78. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the Illinois Consumer Fraud Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT IV
Illinois Personal Information Protection Act,
815 Ill. Comp. Stat. 530/1, *et seq.*
(On Behalf of the Illinois Class)

79. Plaintiff incorporates paragraphs 1–52 as if fully set forth herein.

80. ComplyRight violated 815 Ill. Comp. Stat. 530/10(a) by failing to notify Illinois residents at no charge of the Data Breach in the most expedient time possible and without unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiff and the other Class members until July 13, 2018.

81. Furthermore, the notification was insufficient, misleading, and not compliant with Illinois law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other

media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, the Data Breach failed to accurately and sufficiently identify the relevant data collector.

82. ComplyRight violated 815 Ill. Comp. Stat. 530/45 by failing to implement and maintain reasonable security measures to protect the Personal Information from unauthorized access, acquisition, destruction, use, modification, or disclosure. ComplyRight's security measures were unreasonable and inadequate to prevent or mitigate the scope and duration of the Data Breach, were inadequate to detect the suspicious activity for an unreasonably long period of time, and were unable to ascertain the disposition of vast amounts of sensitive data. These unreasonable security measures caused, facilitated, and exacerbated the Data Breach and the damages that Plaintiff and the other Class members have incurred, are incurring, and will incur as a result of the Data Breach.

83. ComplyRight's PIPA violations constitute unfair or deceptive acts for which Plaintiff has a right of action under 815 Ill. Comp. Stat. 505/10.

84. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

85. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the PIPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

86. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against ComplyRight, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's motion for class certification;

B. Ordering ComplyRight to pay actual damages to Plaintiff and the other Class members;

C. Ordering ComplyRight to pay punitive damages, as allowable by law, to Plaintiff and the other Class members;

D. Ordering ComplyRight to pay Plaintiff's attorneys' fees, costs, and expenses;

E. Ordering ComplyRight to provide equitable relief, in the form of disgorgement and restitution, and injunctive relief;

F. Ordering ComplyRight to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Dated: July 20, 2018

Respectfully submitted,

/s/ Ben Barnow

Ben Barnow
Erich P. Schork
Jeffrey D. Blake
Anthony L. Parkhill
Barnow and Associates, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312)-641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
j.blake@barnowlaw.com
aparkhill@barnowlaw.com

Aron D. Robinson
Law Offices of Aron D. Robinson
180 W. Washington, Suite 700
Chicago, IL 60602
Tel: (312) 857-9050
Fax: (312) 857-9054
adroblaw@aol.com

Attorneys for Plaintiff Susan Winstead